Vulnerability Assessment

Course Introduction

Alexis Ahmed

Senior Penetration Tester
@HackerSploit
Offensive Security Instructor @INE

Course Topic Overview

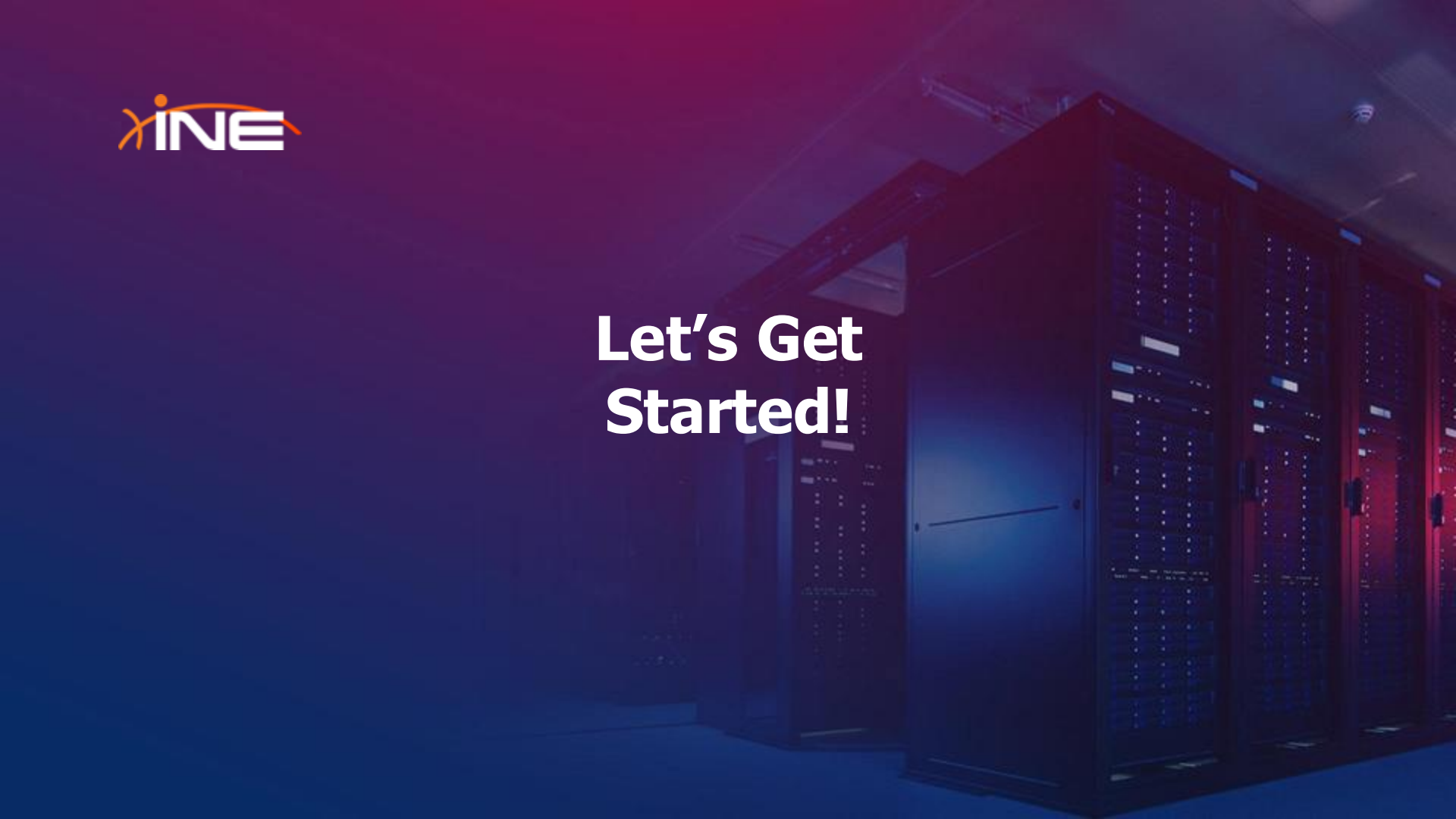
- Introduction To Vulnerability Assessment
- Overview of Windows Vulnerabilities
- Vulnerability Scanning with MSF
- Overview of Linux Vulnerabilities
- Vulnerability Scanning With Nessus

Prerequisites

- Basic Knowledge of Cybersecurity Concepts.
- Basic knowledge of penetration testing methodologies and the penetration testing lifecycle.
- Basic knowledge and experience in using Nmap for host discovery and port scanning.
  - Recommended Course: Assessment Methodologies: Footprinting & Scanning)

Learning Objectives:

- Understand the principles and importance of vulnerability assessment.
- Learn the role of vulnerability assessment in the penetration testing life cycle.
- Identify and differentiate between types of vulnerability scans and scanners.
- Gain hands-on experience with vulnerability scanning tools through practical lab demos.



Let’s Get Started!

Overview Of Windows Vulnerabilities

A Brief History of Windows Vulnerabilities

- Microsoft Windows is the dominant operating system worldwide with a market share >=70% as of 2021.
- The popularity and deployment of Windows by individuals and companies makes it a prime target for attackers given the threat surface.
- Over the last 15 years, Windows has had its fair share of severe vulnerabilities, ranging from MS08-067(Conflicker) to MS17-010 (EternalBlue).
- Given the popularity of Windows, most of these vulnerabilities have publicly accessible exploit code making them relatively straightforward to exploit.

Windows Vulnerabilities

- Microsoft Windows has various OS versions and releases which makes the threat surface fragmented in terms of vulnerabilities. For example, vulnerabilities that exist in Windows 7 are not present in Windows 10.

- Regardless of the various versions and releases, all Windows OS's share a likeness given the development model and philosophy:
  - Windows OS's have been developed in the C programming language, making them vulnerable to buffer overflows, arbitrary code execution etc.
  - By default, Windows is not configured to run securely and require a proactive implementation of security practices in order to configure Windows to run securely.
  - Newly discovered vulnerabilities are not immediately patched by Microsoft and given the fragmented nature of Windows, many systems are left unpatched.

Windows Vulnerabilities

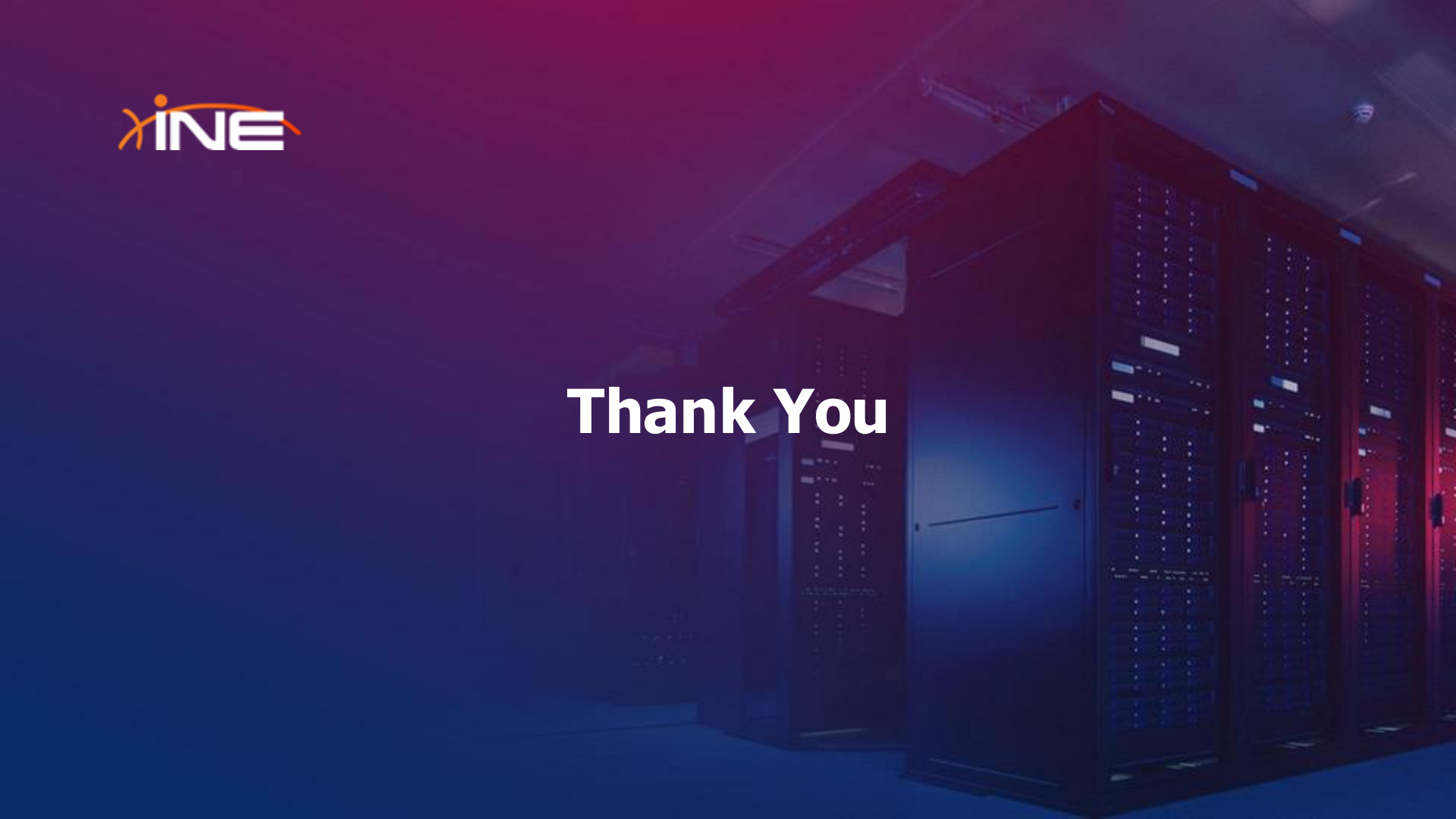
- The frequent releases of new versions of Windows is also a contributing factor to exploitation, as many companies take a substantial length of time to upgrade their systems to the latest version of Windows and opt to use older versions that may be affected by an increasing number of vulnerabilities.

- In addition to inherent vulnerabilities, Windows is also vulnerable to cross platform vulnerabilities, for example SQL injection attacks.

- Systems/hosts running Windows are also vulnerable to physical attacks like; theft, malicious peripheral devices etc.

Types of Windows Vulnerabilities

- Information disclosure - Vulnerability that allows an attacker to access confidential data.
- Buffer overflows - Caused by a programming error, allows attackers to write data to a buffer and overrun the allocated buffer, consequently writing data to allocated memory addresses.
- Remote code execution - Vulnerability that allows an attacker to remotely execute code on the target system.
- Privilege escalation - Vulnerability that allows an attacker to elevate their privileges after initial compromise.
- Denial of Service (DOS) - Vulnerability that allows an attacker to consume a system/host's resources (CPU, RAM, Network etc) consequently preventing the system from functioning normally.


Thank You

Overview Of Windows Vulnerabilities

A Brief History of Windows Vulnerabilities

- Microsoft Windows is the dominant operating system worldwide with a market share >=70% as of 2021.
- The popularity and deployment of Windows by individuals and companies makes it a prime target for attackers given the threat surface.
- Over the last 15 years, Windows has had its fair share of severe vulnerabilities, ranging from MS08-067(Conflicker) to MS17-010 (EternalBlue).
- Given the popularity of Windows, most of these vulnerabilities have publicly accessible exploit code making them relatively straightforward to exploit.

Windows Vulnerabilities

- Microsoft Windows has various OS versions and releases which makes the threat surface fragmented in terms of vulnerabilities. For example, vulnerabilities that exist in Windows 7 are not present in Windows 10.

- Regardless of the various versions and releases, all Windows OS's share a likeness given the development model and philosophy:
  - Windows OS's have been developed in the C programming language, making them vulnerable to buffer overflows, arbitrary code execution etc.
  - By default, Windows is not configured to run securely and require a proactive implementation of security practices in order to configure Windows to run securely.
  - Newly discovered vulnerabilities are not immediately patched by Microsoft and given the fragmented nature of Windows, many systems are left unpatched.

Windows Vulnerabilities

- The frequent releases of new versions of Windows is also a contributing factor to exploitation, as many companies take a substantial length of time to upgrade their systems to the latest version of Windows and opt to use older versions that may be affected by an increasing number of vulnerabilities.

- In addition to inherent vulnerabilities, Windows is also vulnerable to cross platform vulnerabilities, for example SQL injection attacks.

- Systems/hosts running Windows are also vulnerable to physical attacks like; theft, malicious peripheral devices etc.

Types of Windows Vulnerabilities

- Information disclosure - Vulnerability that allows an attacker to access confidential data.
- Buffer overflows - Caused by a programming error, allows attackers to write data to a buffer and overrun the allocated buffer, consequently writing data to allocated memory addresses.
- Remote code execution - Vulnerability that allows an attacker to remotely execute code on the target system.
- Privilege escalation - Vulnerability that allows an attacker to elevate their privileges after initial compromise.
- Denial of Service (DOS) - Vulnerability that allows an attacker to consume a system/host's resources (CPU, RAM, Network etc) consequently preventing the system from functioning normally.

Frequently Exploited Windows Services

Frequently Exploited Windows Services

- Microsoft Windows has various native services and protocols that can be configured to run on a host.
- These services provide an attacker with an access vector that they can utilize to gain access to a target host.
- Having a good understanding of what these services are, how they work and their potential vulnerabilities is a vitally important skill to have as a penetration tester.

Frequently Exploited Windows Services

Protocol/Service	Ports	Purpose
Microsoft IIS (Internet Information Services)	TCP ports 80/443	Proprietary web server software developed by Microsoft that runs on Windows.
WebDAV (Web Distributed Authoring & Versioning)	TCP ports 80/443	HTTP extension that allows clients to update, delete, move and copy files on a web server. WebDAV is used to enable a web server to act as a file server.
SMB/CIFS (Server Message Block Protocol)	TCP port 445	Network file sharing protocol that is used to facilitate the sharing of files and peripherals between computers on a local network (LAN).
RDP(Remote Desktop Protocol)	TCP port 3389	Proprietary GUI remote access protocol developed by Microsoft and is used to remotely authenticate and interact with a Windows system.
WinRM (Windows Remote Management Protocol)	TCP ports 5986/443	Windows remote management protocol that can be used to facilitate remote access with Windows systems.

Vulnerability Scanning With MSF

Vulnerability Scanning

- Vulnerability scanning & detection is the process of scanning a target for vulnerabilities and verifying whether they can be exploited.

- So far, we have been able to identify and exploit misconfigurations on target systems, however, in this section we will be exploring the process of utilizing auxiliary and exploit modules to scan and identify inherent vulnerabilities in services, operating systems and web applications.

- This information will come in handy during the exploitation phase of this course.

- We will also be exploring the process of utilizing third party vulnerability scanning tools like Nessus and how we can integrate Nessus functionality in to the MSF.

Lab Environment

- For the purposes of demonstrating the vulnerability scanning process, we will be utilizing an intentionally vulnerable virtual machine called Metasploitable3 that is based on Windows Server 2008.

- Metasploitable3 was developed by Rapid7 to demonstrate how MSF can be used to perform exploitation of a Windows System.

- Instructions on how this VM can be setup can be found here: https://bit.ly/3kASwns

Demo: Vulnerability Scanning With MSF

WebDAV Vulnerabilities

Microsoft IIS

- IIS (Internet Information Services) is a proprietary extensible web server software developed by Microsoft for use with the Windows NT family.
- It can be used to host websites/web apps and provides administrators with a robust GUI for managing websites.
- IIS can be used to host both static and dynamic web pages developed in ASP.NET and PHP.
- Typically configured to run on ports 80/443.
- Supported executable file extensions:
  - .asp
  - .aspx
  - .config
  - .php

WebDAV

- WebDAV (Web-based Distributed Authoring and Versioning) is a set of extensions to the HTTP protocol which allow users to collaboratively edit and manage files on remote web servers.
- WebDAV essentially enables a web server to function as a file server for collaborative authoring.
- WebDAV runs on top Microsoft IIS on ports 80/443.
- In order to connect to a WebDAV server, you will need to provide legitimate credentials. This is because WebDAV implements authentication in the form of a username and password.

WebDAV Exploitation

- The first step of the exploitation process will involve identifying whether WebDAV has been configured to run on the IIS web server.
- We can perform a brute-force attack on the WebDAV server in order to identify legitimate credentials that we can use for authentication.
- After obtaining legitimate credentials, we can authenticate with the WebDAV server and upload a malicious .asp payload that can be used to execute arbitrary commands or obtain a reverse shell on the target.

Tools

- davtest - Used to scan, authenticate and exploit a WebDAV server.
  + Pre-installed on most offensive penetration testing distributions like Kali and Parrot OS.

- cadaver - cadaver supports file upload, download, on-screen display, in-place editing, namespace operations (move/copy), collection creation and deletion, property manipulation, and resource locking on WebDAV servers.
  + Pre-installed on most offensive penetration testing distributions like Kali and Parrot OS.

Note: All techniques demonstrated in this course are performed on Kali Linux.

Demo: Exploiting Microsoft IIS WebDAV

Vulnerability Analysis: EternalBlue

MS17-010 EternalBlue Exploit

- EternalBlue (MS17-010/CVE-2017-0144) is the name given to a collection of Windows vulnerabilities and exploits that allow attackers to remotely execute arbitrary code and gain access to a Windows system and consequently the network that the target system is a part of.

- The EternalBlue exploit was developed by the NSA (National Security Agency) to take advantage of the MS17-010 vulnerability and was leaked to the public by a hacker group called the Shadow Brokers in 2017.

- The EternalBlue exploit takes advantage of a vulnerability in the Windows SMBv1 protocol that allows attackers to send specially crafted packets that consequently facilitate the execution of arbitrary commands.

MS17-010 EternalBlue Exploit

- The EternalBlue exploit was used in the WannaCry ransomware attack on June 27, 2017 to exploit other Windows systems across networks with the objective of spreading the ransomware to as many systems as possible.

- This vulnerability affects multiple versions of Windows:
  - Windows Vista
  - Windows 7
  - Windows Server 2008
  - Windows 8.1
  - Windows Server 2012
  - Windows 10
  - Windows Server 2016

MS17-010 EternalBlue Exploit

- Microsoft released a patch for the vulnerability in March, 2017, however, many users and companies have still not yet patched their systems.
- The EternalBlue exploit has a MSF auxiliary module that can be used to check if a target system if vulnerable to the exploit and also has an exploit module that can be used to exploit the vulnerability on unpatched systems.
- The EternalBlue exploit module can be used to exploit vulnerable Windows systems and consequently provide us with a privileged meterpreter session on the target system.

Demo: Exploiting Windows MS17-010 SMB Vulnerability

Vulnerability Analysis: BlueKeep

CVE-2019-0708 - BlueKeep

- BlueKeep (CVE-2019-0708) is the name given to an RDP vulnerability in Windows that could potentially allow attackers to remotely execute arbitrary code and gain access to a Windows system and consequently the network that the target system is a part of.

- The BlueKeep vulnerability was made public by Microsoft in May 2019.

- The BlueKeep exploit takes advantage of a vulnerability in the Windows RDP protocol that allows attackers to gain access to a chunk of kernel memory consequently allowing them to remotely execute arbitrary code at the system level without authentication.

CVE-2019-0708 - BlueKeep

- Microsoft released a patch for this vulnerability on May 14th, 2019 and has urged companies to patch this vulnerability as soon as possible.

- At the time of discovery, about 1 million systems worldwide were found to be vulnerable.

- The BlueKeep vulnerability affects multiple versions of Windows:
  - XP
  - Vista
  - Windows 7
  - Windows Server 2008 & R2

CVE-2019-0708 - BlueKeep Exploit

- The BlueKeep vulnerability has various illegitimate PoC's and exploit code that could be malicious in nature. It is therefore recommended to only utilize verified exploit code and modules for exploitation.

- The BlueKeep exploit has an MSF auxiliary module that can be used to check if a target system if vulnerable to the exploit and also has an exploit module that can be used to exploit the vulnerability on unpatched systems.

- The BlueKeep exploit module can be used to exploit vulnerable Windows systems and consequently provide us with a privileged meterpreter session on the target system.

Note: Targeting Kernel space memory and applications can cause system crashes.

Demo: Exploiting Windows CVE-2019-0708 RDP Vulnerability (BlueKeep)

Pass-The-Hash Attacks

Pass-The-Hash

- Pass-the-hash is an exploitation technique that involves capturing or harvesting NTLM hashes or clear-text passwords and utilizing them to authenticate with the target legitimately.

- We can use multiple tools to facilitate a Pass-The-Hash attack:
  - Metasploit PsExec module
  - Crackmapexec

- This technique will allow us to obtain access to the target system via legitimate credentials as opposed to obtaining access via service exploitation.

Demo: Pass-The-Hash Attacks

Frequently Exploited Linux Services

Frequently Exploited Linux Services

- Linux is a free and open source operating system that is comprised of the Linux kernel, which was developed by Linus Torvalds, and the GNU toolkit, which is a collection of software and utilities that was started and developed by Richard Stallman.
- This combination of open source software is what makes up the Linux OS as a whole, and it is commonly referred to as GNU/Linux.
- Linux has various use cases, however, it is typically deployed as a server operating system. For this reason, there are specific services and protocols that will typically be found running on a Linux server.
- These services provide an attacker with an access vector that they can utilize to gain access to a target host.
- Having a good understanding of what these services are, how they work and their potential vulnerabilities is a vitally important skill to have as a penetration tester.

Frequently Exploited Linux Services

Protocol/Service	Ports	Purpose
Apache Web Server	TCP ports 80/443	Free and open source cross-platform web server released under the Apache License 2.0. Apache accounts for over 80% of web servers globally.
SSH (Secure Shell)	TCP ports 22	SSH is a cryptographic remote access protocol that is used to remotely access and control systems over an unsecured network. SSH was developed as a secure successor to telnet.
FTP (File Transfer Protocol)	TCP port 21	FTP (File Transfer Protocol) is a protocol that uses TCP port 21 and is used to facilitate file sharing between a server and client/clients and vice versa.
SAMBA	TCP port 445	Samba is the Linux implementation of SMB, and allows Windows systems to access Linux shares and devices.

Exploiting Bash CVE-2014-6271 Vulnerability (Shellshock)

CVE-2014-6271 - Shellshock

- Shellshock (CVE-2014-6271) is the name given to a family of vulnerabilities in the Bash shell (since V1.3) that allow an attacker to execute remote arbitrary commands via Bash, consequently allowing the attacker to obtain remote access to the target system via a reverse shell.

- The Shellshock vulnerability was discovered by Stéphane Chazelas on the 12th of September 2014 and was made public on the 24th of September 2014.

- Bash is a *Nix shell that is part of the GNU project and is the default shell for most Linux distributions.

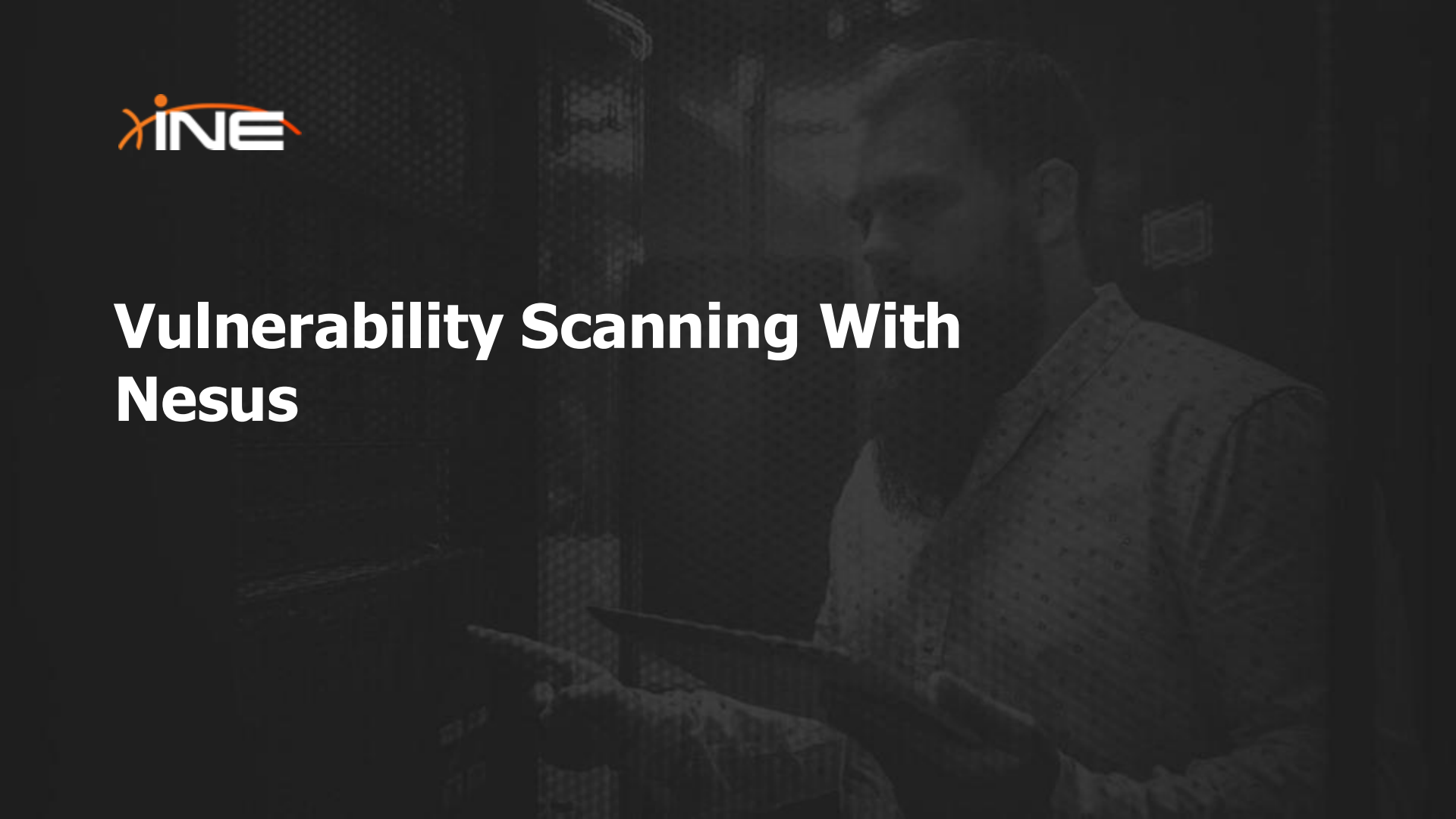
CVE-2014-6271 - Shellshock

- The Shellshock vulnerability is caused by a vulnerability in Bash, whereby Bash mistakenly executes trailing commands after a series of characters: () {:;};.
- This vulnerability only affects Linux as Windows does not use utilize Bash as it is not a *Nix based operating system.
- In the context of remote exploitation, Apache web servers configured to run CGI scripts or .sh scripts are also vulnerable to this attack.
- CGI (Common Gateway Interface) scripts are used by Apache to execute arbitrary commands on the Linux system, after which the output is displayed to the client.

Shellshock Exploitation

- In order to exploit this vulnerability, you will need to locate an input vector or script that allows you to communicate with Bash.
- In the context of an Apache web server, we can utilize any legitimate CGI scripts accessible on the web server.
- Whenever a CGI script is executed, the web server will initiate a new process and run the CGI script with Bash.
- This vulnerability can be exploited both manually and automatically with the use of an MSF exploit module.

Demo: Exploiting Bash CVE-2014-6271 Vulnerability (Shellshock)



Vulnerability Scanning With Nesus

Vulnerability Scanning With Nessus

- Nessus is a proprietary vulnerability scanner developed by Tenable.
- We can utilize Nessus to perform a vulnerability scan on a target system, after which, we can import the Nessus results in to MSF for analysis and exploitation.
- Nessus automates the process of identifying vulnerabilities and also provides us with information pertinent to a vulnerability like the CVE code.
- We can use the free version of Nessus (Nessus Essentials), which allows us to scan upto 16 IPs.

Lab Environment

- For the purposes of demonstrating the vulnerability scanning process, we will be utilizing an intentionally vulnerable virtual machine called Metasploitable3 that is based on Windows Server 2008.

- Metasploitable3 was developed by Rapid7 to demonstrate how MSF can be used to perform exploitation of a Windows System.

- Instructions on how this VM can be setup can be found here: https://bit.ly/3kASwns

Demo: Vulnerability Scanning With Nessus

Web App Vulnerability Scanning

WMAP

- WMAP is a powerful, feature-rich web application vulnerability scanner that can be used to automate web server enumeration and scan web applications for vulnerabilities.
- WMAP is available as an MSF plugin and can be loaded directly into MSF.
- WMAP is fully integrated with MSF, which consequently allows us to perform web app vulnerability scanning from within the MSF.

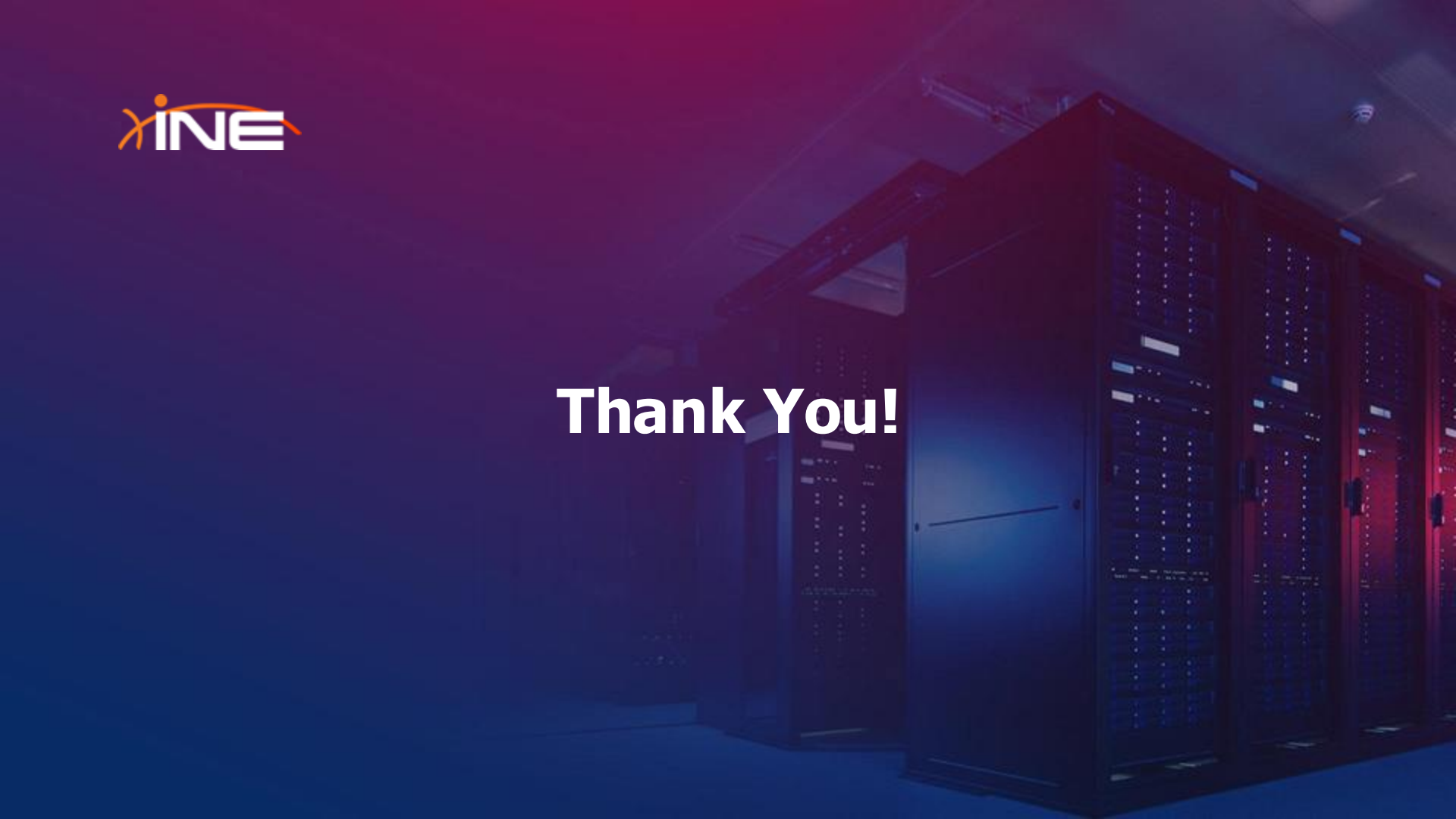
Demo: Web App Vulnerability Scanning With WMAP

Vulnerability Assessment

Course Conclusion

Learning Objectives:

- Understand the principles and importance of vulnerability assessment.
- Learn the role of vulnerability assessment in the penetration testing life cycle.
- Identify and differentiate between types of vulnerability scans and scanners.
- Gain hands-on experience with vulnerability scanning tools through practical lab demos.


Thank You!

EXPERTS AT MAKING YOU AN EXPERT